THE HONORABLE MARSHA J. PECHMAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

WEIMIN CHEN, for Himself, as a Private Attorney General, and/or On Behalf Of All Others Similarly Situated, Plaintiff, v. LAMPS PLUS, INC., and DOES 1-20, inclusive, Defendants.	CASE NO. 2:19-cv-00119-MJP **AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION AND STIPULATED ORDER**

Plaintiff Weimin Chen and Defendant Lamps Plus, Inc. (each a "party" and collectively the "parties") hereby stipulate to — and respectfully request that the Court enter as an Order — the following provisions regarding the discovery of electronically stored information ("ESI") in this matter:

A. General Principles

1. An attorney's zealous representation of a client is not compromised by conducting discovery in a cooperative manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions.

2. The proportionality standard set forth in Fed. R. Civ. P. 26(b)(1) must be applied in each case when formulating a discovery plan. To further the application of the

proportionality standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as possible.

3. If the parties are unable to resolve any dispute regarding ESI or arising under this Order, then the parties shall meet and confer within one week of a meet and confer request by any party, and, if the dispute remains unresolved, the parties will resolve the dispute using the expedited joint motion procedure enunciated in Local Civil Rule 37(a)(2). If requested by any party, the parties shall conduct a meet and confer which includes the parties' technical personnel.

B. Liasons

The parties have identified liaisons to each other who are and will be knowledgeable about and responsible for discussing their respective ESI. Each eDiscovery liaison will be, or have access to those who are, knowledgeable about the technical aspects of eDiscovery, including the location, nature, accessibility, format, collection, search methodologies, and production of ESI in this matter. The parties will rely on the liaisons, as needed, to confer about ESI and to help resolve disputes without court intervention. The eDiscovery liaisons for each of the parties are as follows:

Daniel Hattis dan@hattislaw.com	eDiscovery Liaison for Plaintiffs
Lauren Doucette ldoucette@sheppardmullin.com	eDiscovery Liaison for Defendant

If the parties need to make modifications to their designated eDiscovery Liaisons, the party effecting the changes shall notify all other parties within 5 business days of the change, including the new contact information for the eDiscovery Liaison.

C. ESI Disclosures

Within 30 days of the Court's entry of this stipulation as an Order, each Party shall disclose:

1. Custodians. The six (6) custodians most likely to have discoverable ESI in their possession, custody or control. The custodians shall be identified by name, title, connection to the instant litigation, and the type of the information under his/her control. If discovery indicates the existence of one or more potential additional custodians, the parties shall meet and confer regarding the production of discovery from said custodian(s).

2. Non-custodial Data Sources. A list of non-custodial data sources (e.g. shared drives, servers, etc.), if any, likely to contain discoverable ESI.

3. Third-Party Data Sources. A list of third-party data sources, if any, likely to contain discoverable ESI. E.g., third-party email and/or mobile device providers; third-party cloud storage and third-party cloud applications (e.g. Amazon Web Services; Microsoft Azure Cloud Services; Google Cloud, G Suite Apps, and Google Docs; Microsoft Office 365; or Apple iCloud); messaging products such as Slack, Microsoft Teams, Skype; and, for each such source, the extent to which a party is (or is not) able to preserve information stored in the third-party data source. Third-Party Data Sources shall be further defined as data the party custodians have access to, either through login credentials and/or a subscription service, and not data held by third party custodians that are not under the custody, control, or licensed access of the parties.

4. Inaccessible Data. A list of data sources, if any, likely to contain discoverable ESI (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the data source) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

D. Preservation of ESI

The parties acknowledge that they have a common law obligation to take reasonable and proportional steps to preserve discoverable information in the Party’s possession, custody or control. With respect to preservation of ESI, the parties agree as follows:

1. Absent a showing of good cause by the requesting party, the parties shall not be required to modify the procedures used by them in the ordinary course of business to back-up and archive data; provided, however, that the parties shall preserve all discoverable ESI in their

possession, custody or control.

2. All parties shall supplement their disclosures in accordance with Rule 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made (unless excluded by the Rule or as provided for herein).

3. Absent a showing of good cause by the requesting party, the following categories of ESI need not be preserved:

a. Deleted, slack, fragmented, or other data only accessible by forensics.

b. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

c. Online access data such as temporary internet files, history, cache, cookies, and the like.

d. Data in metadata fields that are frequently updated automatically, such as last-opened dates.

e. Back-up data that are substantially duplicative of data that are more accessible elsewhere.

f. Server, system or network logs.

g. Data remaining from systems no longer in use that is unintelligible on the systems in use.

h. Electronic data (e.g. email, calendars, contact data, and notes) sent to or from mobile devices (e.g., iPhone, iPad, Android, and Blackberry devices), provided that a copy of all such electronic data is routinely saved elsewhere (such as on a server, laptop, desktop computer, or "cloud" storage).

E. Privilege

1. With respect to privileged or work-product information generated after July 5, 2017 (the date of the filing of the complaint in the *Seegert v. Lamps Plus* matter), the parties are not required to include any such information in privilege logs.

2. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).

3. Information produced in discovery that is protected as privileged or work product shall be immediately returned to the producing party, and its production shall not constitute a waiver of such protection, if: (i) such information appears on its face to have been inadvertently produced or (ii) the producing party provides notice within 15 days of discovery by the producing party of the inadvertent production.

4. Privilege Log Based on Metadata. The parties agree that privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged or work-product protection). For ESI, the privilege log must be generated using available metadata, if such metadata is not itself privileged (subject line, file name, etc.). Should the available metadata provide insufficient information for the purpose of evaluating the privilege claim asserted, the producing party shall include such additional information as required by the Federal Rules of Civil Procedure.

F. ESI Discovery Procedures

1. Easily Segregable Documents**.** Documents or categories of documents that are easily identifiable and segregable shall be collected without the use of search terms or other agreed upon advanced search methodology (*e.g.*, analytics, predictive coding, technology-assisted-review). The producing party will indicate which categories of documents will be produced with and without the use of search terms or other advanced search methodology. Where potentially responsive ESI shall be searched through the use of search terms, the parties agree to follow the process identified below and the parties shall meet and confer regarding any proposed deviation.

2. Search Terms. The parties shall timely attempt to reach agreement on appropriate search terms, or an appropriate computer- or technology-aided methodology, before any such effort is undertaken. The parties shall continue to cooperate in revising the appropriateness of the search terms or computer- or technology-aided methodology.

In the absence of agreement on appropriate search terms, or an appropriate computer- or technology-aided methodology, the following procedures shall apply:

a. A producing party shall disclose the search terms or queries, if any, and methodology that it proposes to use to filter ESI likely to contain discoverable information. The parties shall meet and confer to attempt to reach an agreement on the producing party's search terms and/or other methodology.

b. If search terms or queries are used to filter ESI likely to contain discoverable information, a requesting party is entitled to no more than six (6) additional terms or queries to be used in connection with further electronic searches absent a showing of good cause or agreement of the parties. Upon receipt of the full production, the parties may meet and confer on additional search terms if the requesting party feels that additional responsive records exist that were not already produced.

c. Focused terms and queries should be employed; broad terms or queries, such as product and company names, generally should be avoided.

d. The producing party shall search both ESI maintained by the custodians identified above and non-custodial data that the parties can reasonably access and search. The producing party shall not be required to search and extract data from non-custodial data sources that it does not have access to, such as login credentials and/or licenses, and non-custodial data sources that the party custodians do not have a reasonable way to extract data from them, including programs that do not have compliance options/aspects, programs that do not allow the user to export data from the program, and any burdensome extraction processes. These inaccessible non-custodial data sources shall be handled via a third party records subpoena issued by the requesting party.

4. Family Relationships. Family relationships shall be maintained for all responsive records, unless a claim of privilege is being asserted. Families refer to connected records, such as an email (the "parent") with its corresponding attachments (the "children"). If family relationships are severed due to privilege, the producing party shall provide a privilege log

including the name of the individual from whom the privileged document emanated, the name of the individual(s) to whom the allegedly privileged document was directed, the date the document was created, the title of the document or subject line of the document claimed to be privileged, if not privileged content itself, and the privilege claimed and its basis in law, in addition to the corresponding Group Identifier to identify the broken familial relationship from the privilege log.

G. ESI Production

1. <u>Format – Hard Copy Documents</u>

a. Hard copy documents should be scanned as single-page, Group IV, 300 DPI TIFF images with an .opt image cross-reference file and a delimited database load file (*i.e.*, .dat). The database load file should contain the following fields: "BATES BEG," "BATES END," "PAGES," "VOLUME," "CUSTODIAN," "ORGFOLDER," "Confidential Designation," and "OCR." The documents should be logically unitized (*i.e.*, distinct documents shall not be merged into a single record, and single documents shall not be split into multiple records) and be produced in the order in which they are kept in the usual course of business. For any binder, folder, box organization present, the producing party shall provide this information via the field, "OrgFolder" delimited with "/" to note each new sub organization level. If an original document contains color to understand the meaning or content of the document, the document shall be produced as single-page, 300 DPI JPG images with JPG compression and a high quality setting as to not degrade the original image. Multi-page OCR text for each document should also be provided. The OCR software shall maximize text quality over process speed and shall not include bates numbers, unless redactions have been applied. Settings such as "auto-skewing" and "auto-rotation" should be turned on during the OCR process.

2. <u>Format – ESI</u>

a. Images. The parties shall produce documents as single-page black-and-white TIFF images or color JPEG format files imaged at a minimum of 300 dpi, Group IV compression, with the exception of spreadsheet type files, source code, audio, video files, and other files that are unable to be imaged. The parties shall name each TIFF file with a unique name matching the Bates number labeled on the corresponding page, and the parties shall group every 1,000 TIFFs into a new folder. The parties agree not to degrade the searchability of documents as part of the document production process. The searchable, extracted text for redacted documents will be replaced with OCR text. For documents originally created in color, the requesting party may, after reviewing such documents and as reasonably necessary, request that such documents be produced in PNG format or compressed JPG or similar format files. Parties are under no obligation to enhance an image beyond how it was kept in the usual course of business.

If a document is produced in native format, a single-page Bates stamped image slip sheet stating the document has been produced in native format will also be provided. Each native file should be named according to the Bates number it has been assigned, and should be linked directly to its corresponding record in the load file using the NATIVE LINK field.

To the extent that either party believes that specific documents orclasses of documents not already identified within this protocol, should be produced in native format the parties agree to meet and confer in good faith.

b. Metadata. For each responsive ESI record that is produced, the parties shall produce extracted metadata in the form of a .dat file along with standard Concordance image load file, and the produced metadata shall include the fields listed in Table I (except that, if the field contains privileged information, that privileged information may be redacted, with any redactions for privilege reasons being recorded on a privilege log).

c. Document Text. Each party shall produce the full text of each electronic document provided in searchable ASCII text format (or Unicode text format if the text is in a foreign language), named with a unique Bates number. For records that contain no redactions, the parties shall produce the extracted text associated with each record. For records that contain redactions, the parties shall produce OCR text for only records containing redactions (not the entire production set) to remove the redacted text from the text file. The text of the document shall not be included in the .dat file, but instead the .dat file shall include a link to the .txt file. Any redacted material should be clearly labeled to show the redactions on the tiff image.

d. Image Load File. Documents shall be produced with appropriate accompanying Concordance load files. The Concordance load files will contain the path to the extracted text files or the native file and all metadata fields contained in Table I. The text of the document shall not be included in the .dat file, but instead the .dat file shall include a link to the .txt file. For images, the parties will provide .OPT (Opticon) files.

e. Records Unable to be Imaged. Responsive documents that are unable to be imaged shall be produced natively with a placeholder image referencing the native file's bates number, that will correspond with the native file's file name. The load file will link the native file with the Bates stamped placeholder and all relevant metadata as listed in Table I. Such responsive documents to be produced natively include video files, audio files, database files, CAD drawings, Excel spreadsheets, and other files that the parties may agree to produce natively through the meet and confer process.

f. Compressed Files Types. Compressed file types (*i.e.* .ZIP, .RAR, .CAB, .Z) should be decompressed so that the lowest level document or file is extracted.

g. De-Duplication. Each party shall remove exact duplicate documents based on MD5 or SHA-1 hash values, at the family level. Attachments should not be eliminated as duplicates for purposes of production, unless the parent e-mail and all attachments are also duplicates. Parties agree that an email that includes content in the BCC or other blind copy field shall not be treated as a duplicate of an email that does not include content in those fields, even if all remaining content in the email is identical. Removal of near-duplicate documents and e-mail thread suppression is not acceptable. De-duplication will be done across the entire collection (global de-duplication) and the Custodian Other field will list each custodian, separated by a semi-colon, who was a source of that document. Should the Custodian Other metadata field produced become outdated due to rolling productions, an overlay file providing all the custodians and file paths for the affected documents will be produced prior to substantial completion of the document production.

The parties may use software to identify and suppress lesser inclusive email threads (i.e., email threads that are contained entirely within a subsequent email thread) and are not required to produce lesser inclusive email threads as long they are produced as part of a longer inclusive email thread. However, the parties are required to preserve all suppressed documents and to produce in their entirety all lesser inclusive emails with attachments that are not part of the more inclusive email thread, and any tangential email threads.

The parties agree that an email that includes content on the “bcc” or other blind copy field shall not be treated as duplicate of an email that does not include content in the “bcc” or other blind copy field, even if all remaining content in the email is identical. The parties will produce a single unique copy of a given e-mail message and its attachments, or standalone file, with references to each custodian/location in which a copy originally appeared as set forth in the metadata specifications above. In the case of duplicates maintained by custodians in different time zones, it is understood that the image and date/time metadata will reflect Pacific Standard Time (“PST”).

3. Structured Data

To the extent a response to discovery requires production of electronic information stored in a database, including the production of sales audit information, pricing information, customer information, text messages or similar communications, the Producing Party shall provide the relevant information extracted from the structured data set in useable reports. The producing party shall provide all responsive records in a useable format, i.e., in a structured dataset, in a way that does not require the requesting party to have a proprietary license to view the records. I.e., to the maximum extent possible, the database information shall be exported in a standard .csv or SQL format so that the requesting party can import and manage the records in a structured database.

4. Transfer of Productions.

To maximize the security of information in transit, any media on which documents are produced may be encrypted. In such cases, the producing party shall transmit the encryption key or password to the receiving party, under separate cover, contemporaneously with sending the encrypted media. Productions not produced on physical media shall be transmitted via sFTP or other file transfer protocol that encrypts documents while in motion and at rest.

With respect to large data productions (such as the production of customer and transactional data), the parties shall meet and confer as necessary regarding the format and logistics of the production, including as necessary conducting calls among the parties' technical personnel.

TABLE I

Field	**Description**
Bates_Begin	The Bates label of the first page of the document
Bates_End	The Bates label of the last page of the document
Attach_Begin	The Bates label of the first page of a family of documents (e.g., email and attachment)
Attach_End	The Bates label of the last page of a family of documents
File Name	The filename of an attachment or stand-alone e-file
File Extension	The file extension of the document (e.g., .doc, .xls)
Subject	The subject of an email
Time_Zone	The time zone used to process the document
Sent_Date	For email, the sent date of the message
Sent_Time	For email, the sent time of the message
Received Date	For email, the date the message was received
Received Time	For email, the time the message was received
Message_ID	For email, the message ID
Create_Date	For efiles or attachments, the document's creation date or operating system creation date
Create_Time	For efiles or attachments, the document's creation time or operating system creation time

Field	Description
Modified_Date	For efiles or attachments, document’s last modified date or operating system last modified date
Modified_Time	For efiles or attachments, the document’s last modified time or operating system last modified time
Author	The author of a stand-alone efile or attachment
From	The sender of an email message
To	The recipients of an email message, in a semi-colon delimited multi-value list
CC	The copyee(s) of an email message, in a semi-colon delimited multi-value list
BCC	The blind copyee(s) of an email message, in a semi-colon delimited, multi-value list
Custodian	The custodian in whose file the document was found
Custodian Other	The custodians of any duplicates, in a semi-colon delimited multi-value list
Modified_Author	The author who last modified the document
MD5 Hash	The calculated MD5 hash value of the document
Native_Link	The file path to the location of the native file if produced natively
OCR/Txt Path	The relative path to the OCR/Txt Files
Redaction	Whether the document is redacted (Yes/No)
Confidential Designation	The confidentiality designation, if any, for the document pursuant to any protective order in the case
OrgFolder	The organizational structure for paper records, to be delimited to show sub-organizational structure as applicable.
Pages	Number of pages per document
Parent ID	Parent control number or parent bates stamp number (this field should only be populated to children, not to the parent itself)

ORDER

Based on the foregoing,

IT IS SO ORDERED.

DATED: May 21, 2019

Marsha J. Pechman
United States District Judge